Amendments to the Specification

Please amend the Abstract of the Disclosure as follows:

~~The present invention provides methods for sending a~~ A digital message is sent from a sender to a recipient in a public-key based cryptosystem comprising an authorizer. The authorizer can be a single entity or comprise a hierarchical or distributed entity. ~~The present invention allows communication of messages by an efficient protocol, not~~ In some embodiments, no ~~involving~~ key status queries or key escrow are needed. ~~, where a message~~ The recipient can decrypt ~~a message from a~~ the message ~~sender~~ only if the recipient possesses up-to-date authority from the authorizer. Other features are also provided. ~~The invention allows such communications in a system comprising a large number (e.g. millions) of users.~~

Please amend the paragraphs numbered below as shown.

[13]   The concept of an identity-based cryptosystem was proposed in A. Shamir, *Identity-Based Cryptosystems and Signatures Schemes*, ADVANCES IN CRYPTOGRAPHY--CRYPTO '84, Lecture Notes in Computer Science 196 (1984), Springer, 47-53. However, practical identity-based encryption schemes have not been found until recently. For instance, identity-based schemes were proposed in C. Cocks, *An Identity-Based Encryption Scheme Based on Quadratic Residues*, available at ~~http://www.cesqg.gov.uk/technology/id-pkc/media/ciren.pdf~~ h-t-t-p://www.cesqg.gov.uk/technology/id-pkc/media/ciren.pdf; D. Boneh, M. Franklin, *Identity Based Encryption from the Weil Pairing*, ADVANCES IN CRYPTOLOGY--CRYPTO 2001, Lecture Notes in Computer Science 2139 (2001), Springer, 213-229; and D. Boneh, M. Franklin, *Identity Based Encryption from the Weil Pairing* (extended version), available at ~~http://www.cs.stanford.edu/~dabo/papers/ibe.pdf~~ h-t-t-p://www.cs.stanford.edu/~dabo/papers/ibe.pdf. Cocks' scheme is based on the "Quadratic Residuosity Problem," and although encryption and decryption are reasonably fast (about the speed of RSA), there is significant message expansion (*i.e.*, the bit-length of the ciphertext is many times the bit-length of the plaintext). The Boneh-Franklin scheme bases its security on the "Bilinear Diffie-Hellman Problem," and it is quite fast and efficient when using Weil or Tate pairings on supersingular elliptic curves or abelian varieties.

[130] In another embodiment of the present invention, a scheme may be used to compress signatures on any type of information in an authorization chain to a single point, i.e. given n signatures on n distinct messages from n distinct users, it is possible to aggregate all these signatures into a single short signature. D. Boneh, C. Gentry and B. Lynn and H. Shacham, *Aggregate and Verifiably Encrypted Signatures from Bilinear Maps*, eprint archive, 2002, available at ~~http://eprint.iacr.org/2002/175/~~ h-t-t-p://eprint.iacr.org/2002/175/ describe a bandwidth-efficient aggregate signature scheme in which multiple signatures by multiple signers on multiple documents may be compactly represented as a single point on an elliptic curve.

[143] In a conventional forward-secure encryption scheme, the lifetime of the system is divided into a number of time-periods, each defining a key validity period. This period is equivalent to the validity period of the identity-based decryption key in a CBE system. In the forward-secure system, the private key changes during successive time periods in such a way that, if the key is compromised, an attacker cannot decrypt messages sent to the recipient in previous time periods. However, if the sender continues to use the key after compromise, the attacker can decrypt messages sent in subsequent time periods. J. Katz, *A Forward-Secure Public-Key Encryption Scheme*, eprint archive, 2002, available at ~~http://eprint.iacr.org/2002/060/~~ h-t-t-p://eprint.iacr.org/2002/060/, the contents of which are incorporated by this reference, describes such a forward-secure scheme. The security of the Katz scheme is based on the bilinear Diffie-Hellman assumption in the random oracle model and may be extended to achieve chosen-ciphertext security.